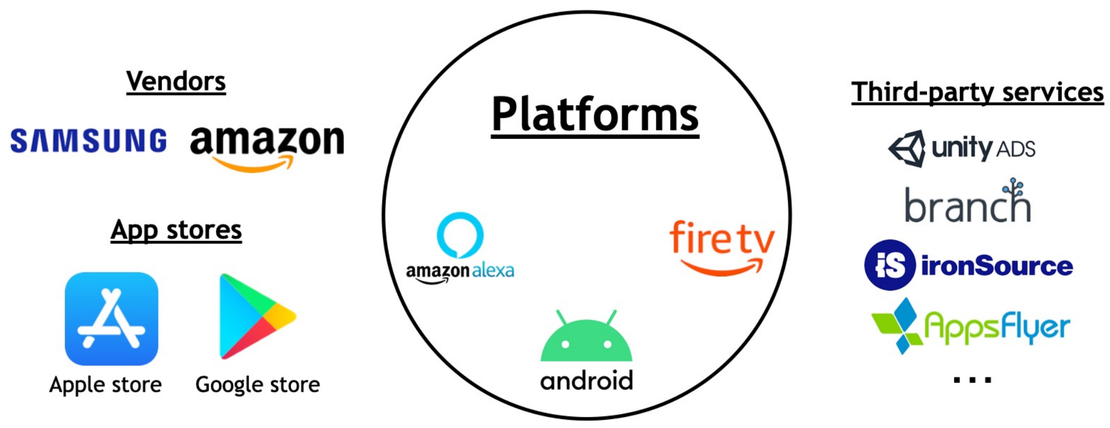
Impostor: Towards an extensible privacy analysis framework for smart homes

Aniketh Girish*#, Juan Tapiador #, Srdjan Matic§, Narseo Vallina-Rodriguez*†

*IMDEA Networks, §IMDEA Software, #Universidad Carlos III de Madrid, † AppCensus

1. IoT Ecosystem

IoT ecosystems are complex entities. They react to external stimuli, from the ***environment***, from ***users*** or other ***devices*** and ***platforms*** co-located in the same local network.



2. Motivation

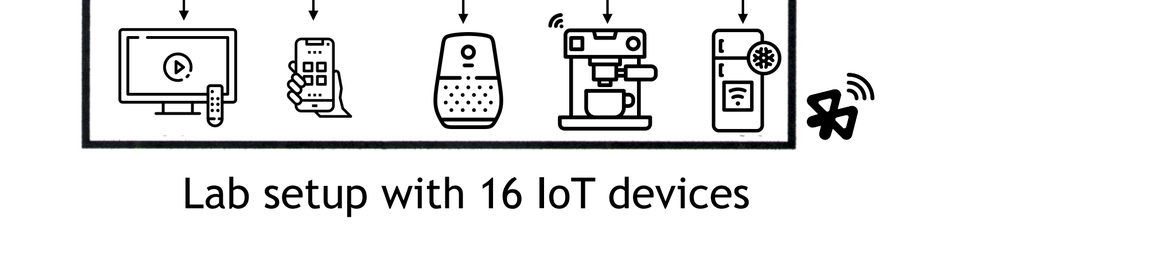
1. Strong privacy regulation exists (e.g., GDPR, CCPA).
2. Certification programs offered by **European commission**, **NIST** and **ioXt** to *secure* consumer-facing IoT endpoints.

Prior work: "IoT devices can be modelled as **monolithic** and **self-contained** entities that communicate *only* with the **cloud**."

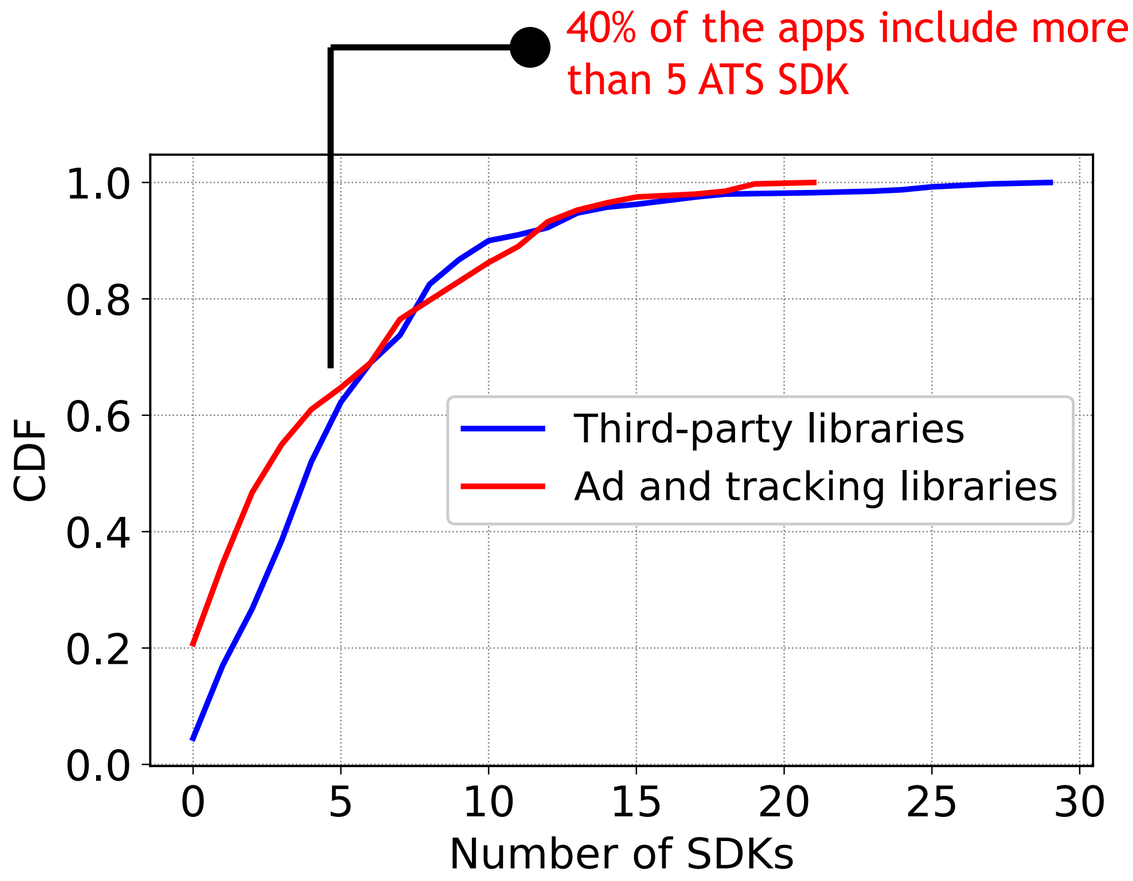
3. Research Questions

1. What behaviours do smart devices exhibit in any arbitrary rich execution environments with a multitude of components and non-deterministic inputs?
2. Do they collude with each other? what are the repercussions of such interactions on user's privacy?

4. Dataset



6. Results



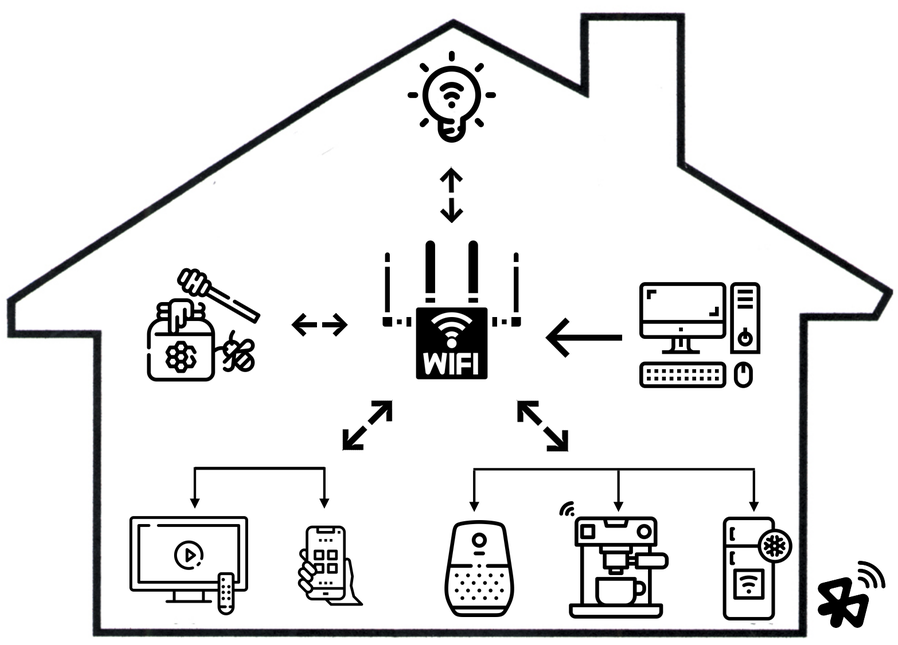
Identifier type	Description
Android ID	Persistent ID created at Android setup
Device ID	Persistent device ID
Advertising ID	Resettable Advertising ID
Serial number	Persistent hardware/manufacturer ID
Router SSID	SSID of the access point

- Discovery protocols share *unique device-specific* values (i.e., device names, serial number, mac addresses)
- Amazon devices communicate with each other using UDP:55444.
  - legitimate use: Synchronizing time.
  - Possible abuse: *Spatial perception*.

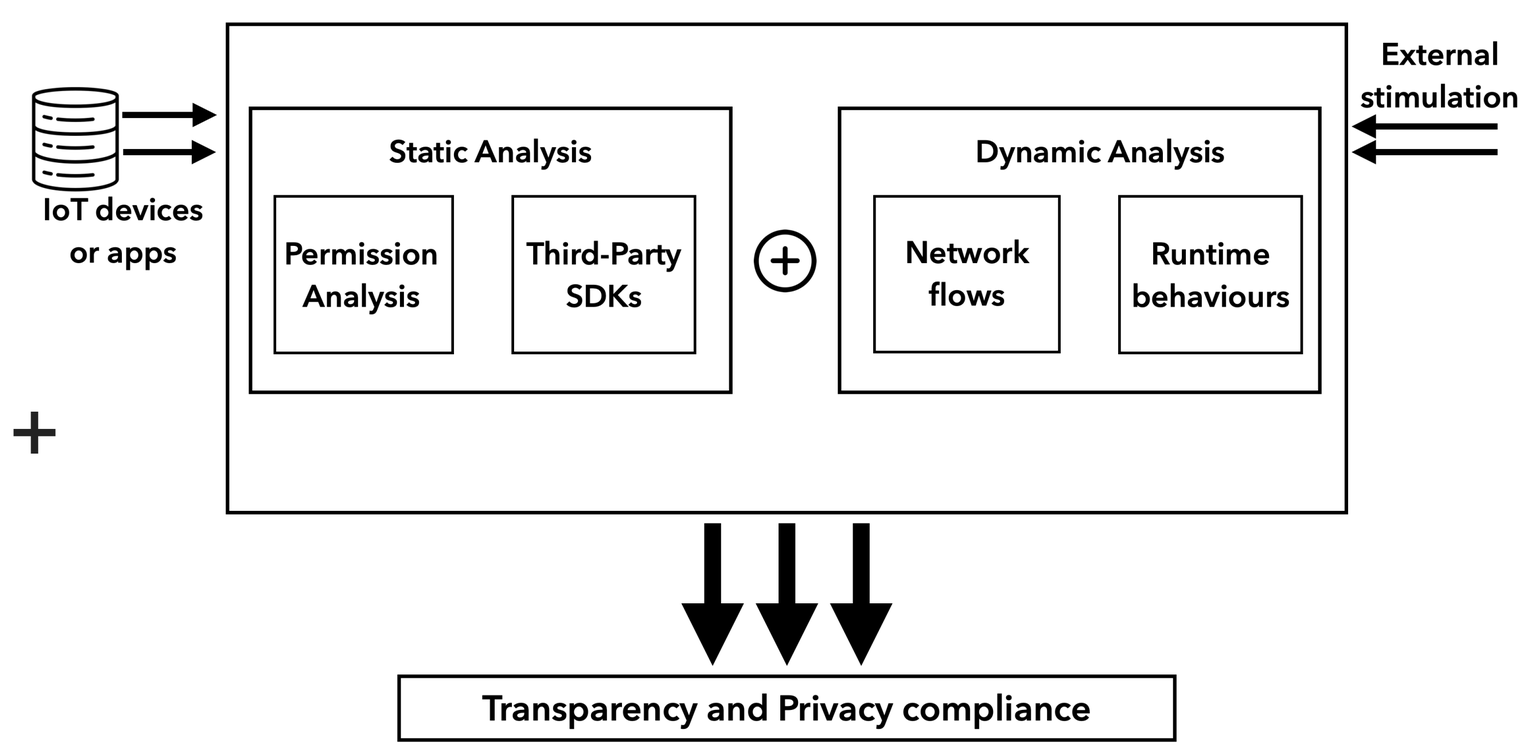
Acknowledgement

This project has been funded by the EU's H2020 Program (TRUST aWARE Project, Grant Agreement No. 101021377) and the Spanish Ministry of Science (ODIO Project, PID2019-111429RB-C22); The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect those of any of the funders.

5. Testbed and empirical Analysis



Lab setup with 16 IoT devices



© Institute IMDEA Networks